18/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011215591 **Image available**
WPI Acc No: 1997-193516/199718
XRPX Acc No: N97-159806

Mutual authentication **of identified** chip cards **with computer system - involves exchange of two random numbers and use of secret OFFSET prior to reciprocal acknowledgement of agreed results of encryption**

Patent Assignee: INFORMATIKZENTRUM SPARKASSENORGANISATION (INFO-N)
Inventor: LOEHMANN E
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 19523466	C1	19970403	DE 1023466	A	19950628	199718	B

Priority Applications (No Type Date): DE 1023466 A 19950628
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 19523466	C1		9	H04L-009/32	

Abstract (Basic): DE 19523466 C

The **chip card** (CC) transmits an **application** (LOG) to the system (S), which returns a random number (RNS) for use with a key (K) in computing a result of encryption (V(K,RNS)). The **chip card** also determines a secret number (OFFSET) for later use and computes another result (V(K,OFFSET)). Both results are transmitted with the identifier (ID) to the system, which derives the key by an established method (F1). The first encryption result is also computed and compared with that from the **chip card** . On receipt of an acknowledgment (OK) the **chip card** sends another random number (RNC), to which the system adds the OFFSET. If the **chip card** agrees with the result, the **application** is authorised.

ADVANTAGE - Simulation of system with fraudulent intent is prevented by multiple use of common identifier.

Dwg.1/4

Title Terms: MUTUAL; AUTHENTICITY; IDENTIFY; CHIP; CARD; COMPUTER; SYSTEM; EXCHANGE; TWO; RANDOM; NUMBER; SECRET; OFFSET; PRIOR; RECIPROCAL; ACKNOWLEDGE; AGREE; RESULT; ENCRYPTION
Derwent Class: T04; W01
International Patent Class (Main): **H04L-009/32**
International Patent Class (Additional): **G06F-012/14** ; G07C-009/00
File Segment: EPI

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 195 23 466 C 1**

(51) Int. Cl.[6]:
H 04 L 9/32
G 06 F 12/14
G 07 C 9/00

(21) Aktenzeichen: 195 23 466.9-31
(22) Anmeldetag: 28. 6. 95
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 3. 4. 97

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Informatikzentrum der Sparkassenorganisation GmbH, 53227 Bonn, DE

(74) Vertreter:
Patentanwälte von Kreisler, Selting, Werner et col., 50667 Köln

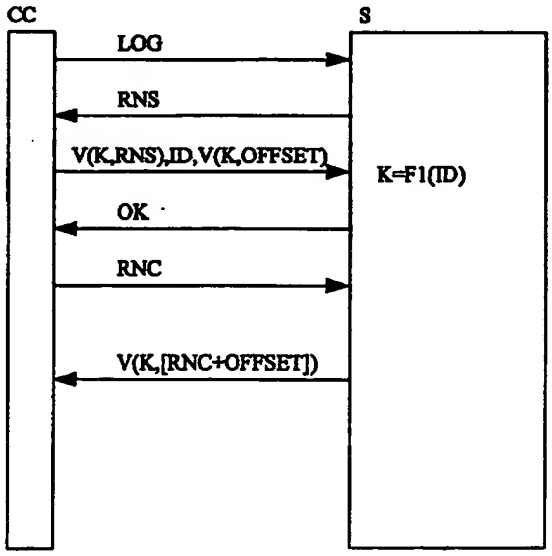
(72) Erfinder:
Löhmann, Ekkehard, 85737 Ismaning, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE	43 42 641 A1
DE	41 38 881 A1
US	52 02 921
EP	0 77 238 B1
EP	5 73 245 A2

(54) **Verfahren zur gegenseitigen Authentifikation von elektronischen Partnern mit einem Rechnersystem**

(57) Bei dem Verfahren zur gegenseitigen Authentifikation eines elektronischen Partners (CC) nach der "Challenge and Response"-Methode mit einem System (S) wird zur Authentifikation des Systems (S) gegenüber dem elektronischen Partner (CC) von dem System (S) auf der Basis der von dem elektronischen Partner (CC) gelieferten zweiten Zufallszahl (RNC) und einem Geheimcode (OFFSET), der ausschließlich dem System (S) und dem elektronischen Partner (CC) bekannt ist, mittels eines Schlüssels (K) ein Verschlüsselungsergebnis errechnet, das an den elektronischen Partner (CC) zurückgesandt wird. Der elektronische Partner (CC) errechnet seinerseits auf der Grundlage ebenfalls der Zufallszahl (RNC) und dem Geheimcode (OFFSET) sowie dem Schlüssel (K) ein Verschlüsselungsergebnis. Erst dann, wenn diese beiden Verschlüsselungsergebnisse übereinstimmen, gilt das System (S) gegenüber dem elektronischen Partner (CC) als authentisch.



DE 195 23 466 C 1

DE 195 23 466 C 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur gegenseitigen Authentifikation eines elektronischen Partners nach der "Challenge and Response" Methode mit einem System gemäß dem Oberbegriff des Anspruchs 1, wie z. B. aus DE 41 38 861 A1 bekannt.

Um Zugang zu einem System zu erhalten, muß häufig die Berechtigung zu diesem Zugang nachgewiesen werden. Andererseits muß sich auch das System eindeutig als echt zu erkennen geben, um einen möglichen Betrug durch ein simuliertes System auszuschließen. Um dies zu gewährleisten, wurde die sogenannten "Challenge and Response"-Methode entwickelt.

Bei dieser Methode schickt zunächst das System eine Zufallszahl an den elektronischen Partner. Dieser verschlüsselt diese Zufallszahl mit einem Verschlüsselungsalgorithmus sowie einem Schlüssel und sendet das Ergebnis gemeinsam mit einer Identitätskenngröße zurück an das System. Mittels eines nur dem System bekannten Verfahrens errechnet das System aus der Identitätskenngröße den Schlüssel und errechnet ebenfalls das Ergebnis, das sich mit Hilfe des Verschlüsselungsalgorithmus aus der Zufallszahl und dem Schlüssel ergibt. Stimmt das vom elektronischen Partner gesendete Ergebnis mit dem vom System errechneten überein, gilt der elektronische Partner als authentisch.

Zur Authentisierung des Systems gegenüber dem elektronischen Partner wird der oben beschriebene Vorgang mit vertauschten Rollen nochmals durchgeführt. Der elektronische Partner sendet eine Zufallszahl zum System, das System verschlüsselt diese Zufallszahl anhand des Verschlüsselungsalgorithmus und des ihm bereits bekannten Schlüssels und sendet das Ergebnis zum Vergleich an den elektronischen Partner.

Der Schlüssel ist demnach lediglich beim elektronischen Partner gespeichert, während das System diesen Schlüssel immer wieder neu nach einem nur dem System bekannten Verfahren unter Zugrundelegen der Identitätskenngröße des elektronischen Partner erzeugen muß. Diese Identitätskenngröße wird während der Initialisierungsphase (Personalisierung), d. h. vor dem erstmaligen Betrieb des Systems gemeinsam mit den elektronischen Partnern, für die elektronischen Partner festgelegt. Dabei erscheint es häufig sinnvoll, ganzen Gruppen von elektronischen Partnern die gleiche Identitätskenngröße und damit auch den gleichen Schlüssel zuzuordnen, um den elektrischen Partnern einer Gruppe die gleichen Zugriffs- und Zugangsrechte zu einem elektronischen Medium zu verleihen.

Aufgrund dieser Praxis ergibt sich aber für einen Betrüger die Möglichkeit, das System bei dessen Authentifikation gegenüber dem elektronischen Partner zu simulieren. Voraussetzung ist lediglich, daß zwei elektronische Partner mit gleicher Identitätskenngröße annähernd gleichzeitig auf das System zugreifen wollen. Die Simulation des Systems kann dann auf folgende Weise durchgeführt werden.

Das simulierende System sendet eine Zufallszahl zum ersten elektronischen Partner, dieser verschlüsselt die Zufallszahl in oben beschriebener Weise und sendet das Ergebnis gemeinsam mit der Identitätskenngröße zum simulierenden System. Dieses bestätigt die Richtigkeit des Ergebnisses, ohne es wirklich überprüft zu haben, woraufhin der erste elektronische Partner seine Zufallszahl zum simulierten System sendet. Dieses reicht die soeben empfangene Zufallszahl an einen ebenfalls gerade auf das System zugreifen wollenden zweiten elektronischen Partner weiter, der daraus — als Teil seiner Authentifikationsprozedur gegenüber dem System — in oben beschriebener Weise das benötigte Verschlüsselungsergebnis berechnet und es an das simulierte System überträgt. Das simulierte System reicht dieses Ergebnis (das mithin von einem elektronischen Partner erzeugt worden ist, der der gleichen Gruppe von Identitätskenngrößen gehört und damit über den gleichen Schlüssel verfügt) zum ersten elektronischen Partner weiter, der es mit dem selbst errechneten Ergebnis vergleicht und die Authentizität des simulierten Systems feststellt. Der zweite elektronische Partner wird durch Übertragung einer Fehlermeldung vom simulierten System abgewiesen.

In DE 41 38 861 A1 wird zwar gezeigt, wie eine Simulation des Systems in betrügerischer Absicht zu verhindern ist; dabei wird jedoch die Eingangsprämisse, nämlich, daß allen elektronischen Partner einer Gruppe die gleiche Identitätsgröße und damit der gleiche Schlüssel zugeordnet wird, durch die Einführung einer individuellen Zusatzidentitätskenngröße verletzt. Diese individuelle Zusatzidentitätskenngröße ist im elektronischen Partner fest abgespeichert.

Die der vorliegenden Erfindung zugrundeliegende Aufgabe ist es nun, bei mehrfacher Verwendung einer gemeinsamen Identitätskenngröße für mehrere elektronische Partner, die gleichzeitig an ein System angeschlossen sein können, eine Simulation des Systems in betrügerischer Absicht zu verhindern.

Diese Aufgabe wird erfindungsgemäß durch die im Patentanspruch 1 angegebenen Merkmale gelöst, und zwar ohne Verletzung der oben genannten Prämisse. Vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens sind jeweils in den Unteransprüchen aufgeführt.

Nach der Erfindung wird der zusätzlich vergebene Geheimcode jedesmal erzeugt, wenn er zur Authentifikation des Systems gegenüber dem elektronischen Partner benötigt wird, wobei es grundsätzlich denkbar ist, daß bei jeder Generierung ein anderer Geheimcode entsteht. Damit kann die Eingangsprämisse, daß eine Gruppe elektronischer Partner mit gleicher Zugriffs- bzw. Zugangsberechtigung mit Ausnahme der Identitätskenngröße keine weiteren Individualisierungskenndaten, insbesondere keine die elektronischen Partner dieser Gruppe untereinander unterscheidenden Individualisierungskenndaten aufweisen, beibehalten werden. Erfindungsgemäß wird der Geheimcode mit der vom elektronischen Partner übermittelten Geheimzahl mathematisch verknüpft. Dabei stellt der Geheimcode ein Geheimnis dar, das lediglich einem elektronischen Partner und nach Versendung dem System bekannt ist.

Durch die erfindungsgemäße Erweiterung des Challenge Response Protokolls kann in vorteilhafter Weise für jeden einzelnen elektronischen Partner ein Austausch von Zufallszahlen mit dem System erreicht werden, so daß danach zweifelsfrei sowohl die Identität des elektronischen Partners als auch die Identität des Systems feststeht, ohne daß dies durch die quasi zeitgleiche Anmeldung eines weitern elektronischen Partners gefährdet wäre.

Damit kann im Falle der Zusammenfassung von elektronischen Partnern in Gruppen mit identischen Identitätskenngrößen einer betrügerischen Simulation des Systems gegenüber einem elektronischen Partner erfolgreich begegnet werden.

Nachfolgend werden anhand der Zeichnung Ausführungsbeispiele der Erfindung näher erläutert. Im einzel-

nen zeigen:

Fig. 1 bis 3 alternative Ausführungsbeispiele des erfindungsgemäßen Verfahrens und

Fig. 4 den Verfahrensablauf bei simuliertem System.

Im folgenden wird anstelle des Begriffes "elektronischer Partner", der für ein beliebig ausgeformtes elektronisches Gerät mit den Fähigkeiten einer Chipkarte steht, der Begriff "Chipkarte" verwendet.

Am linken Rand der Fig. 4 ist symbolisch eine erste Chipkarte CC1 und am rechten Rand symbolisch eine zweite Chipkarte CC2 gezeigt. Zwischen den beiden Chipkarten CC1, CC2 ist symbolisiert durch ein Rechteck ein simuliertes System SS abgebildet. Zu einem bestimmten Zeitpunkt wird beispielsweise durch Einstekken der ersten Chipkarte CC1 in ein Kartenlesegerät die erste Chipkarte CC1 mit dem simulierten System SS verbunden. Die erste Chipkarte CC1 überträgt an das simulierte System SS eine Anmeldeinformation LOG. Daraufhin überträgt das simulierte System SS eine erste Zufallszahl RNS zur ersten Chipkarte CC1. Diese verschlüsselt anhand des Verschlüsselungsalgorithmus V und des in der Karte gespeicherten Schlüssels K die erste Zufallszahl RNS. Das Verschlüsselungsergebnis V (K, RNS) und die in der ersten Chipkarte CC1 gespeicherte Identitätsnummer ID werden zum simulierten System SS übertragen. Das simulierte System SS überträgt ein Quittungssignal OK an die erste Chipkarte CC1. Die erste Chipkarte CC1 interpretiert das Quittungssignal OK so, als wäre der Authentifizierungsprozeß der ersten Chipkarte CC1 gegenüber dem simulierten System SS erfolgreich verlaufen. Deshalb sendet die erste Chipkarte CC1 zur Authentizitätsprüfung des simulierten Systems SS eine zweite Zufallszahl RNC zum simulierten System SS.

Wird nun gleichzeitig oder annähernd gleichzeitig eine zweite Chipkarte CC2, beispielsweise durch Einschieben in ein weiteres Kartenlesegerät mit dem simulierten System SS verbunden, so ergibt sich für den Fall, daß die zweite Chipkarte CC2 die gleiche Identitätskenngröße ID wie die erste Chipkarte CC1 hat die folgende Situation: Zunächst meldet sich auch die zweite Chipkarte CC2 durch Übertragen einer Anmeldeinformation LOG beim simulierten System SS an. Das simulierte System SS reicht nun die von der ersten Chipkarte CC1 empfangene zweite Zufallszahl RNC an die zweite Chipkarte CC2 weiter. Die zweite Chipkarte CC2 verschlüsselt die durchgereichte Zufallszahl RNC mit Hilfe des Verschlüsselungsalgorithmus V und des Schlüssels K und gibt das Verschlüsselungsergebnis V (K, RNC) und die Identitätsnummer ID zum simulierten System SS. zurück. Das simulierte System SS verfügt nun über das zur Authentifikation gegenüber der ersten Chipkarte CC1 erforderliche Verschlüsselungsergebnis V (K, RNC) und überträgt dieses zur ersten Chipkarte CC1. Die gegenseitige Authentifikation zwischen erster Chipkarte CC1 und simuliertem System SS ist damit erfolgreich abgeschlossen. Die zweite Chipkarte CC2 erhält ein negatives Quittungssignal F und wird damit abgewiesen.

In Fig. 1 bis 3 wird nun aufgezeigt, wie die oben beschriebene Authentifikation eines simulierten und damit unberechtigten Systems SS gegenüber einer Chipkarte CC wirksam verhindert werden kann.

Dazu wird das Protokoll so abgeändert, daß bei der Authentifikation des Systems S gegenüber dem elektronischen Partner CC ein zusätzlicher Geheimcode OFFSET (nachfolgend auch geheime Zahl genannt), der dem elektronischen Partner CC zum Zeitpunkt der Initialisierung und dem System S zum Zeitpunkt der Authentifikation bekannt ist, verwendet werden kann. Der Geheimcode OFFSET ist jedoch für alle elektronischen Partner mit derselben Identitätskenngröße gleich.

Auf die Challenge des elektronischen Partners CC (Senden der Zufallszahl RNC) reagiert das System durch Senden des verschlüsselten Wertes von RNC plus OFFSET.

Der relevante Geheimcode OFFSET wird entweder dem System S vom elektronischen Partner als Teil seiner Response auf die Challenge des System (siehe Fig. 1) oder in einem zusätzlichen Protokollschritt verschlüsselt übermittelt, der zwischen der Authentifikation des elektronischen Partners CC und der Authentifikation des Systems liegt, dem System verschlüsselt vom elektronischen Partner CC übermittelt (siehe Fig. 2) oder der die geheime Zahl OFFSET wird bereits zum Zeitpunkt der Initialisierung mit einem geheimen Verfahren F2 aus der Identitätskenngröße ID berechnet und analog zum Schlüssel K beim elektronischen Partner CC gespeichert, wobei der Geheimcode OFFSET im Zuge der Authentifikation des Systems S vom System S aus der übermittelten Identitätsgröße mittels des geheimen Verfahrens F2 jeweils neu berechnet wird (siehe Fig. 3).

Die gegenseitige Authentifikation zwischen Chipkarte CC und System S verläuft dann in Fig. 1 wie folgt:
Die Chipkarte CC überträgt eine Anmeldeinformation LOG an das System S. Das System S erzeugt eine Zufallszahl RNS und überträgt diese an die Chipkarte CC. Die Chipkarte errechnet aus dem Schlüssel K und der Zufallszahl RNS ein Verschlüsselungsergebnis V (K, RNS). Außerdem bestimmt die Chipkarte den später zu verwendenden OFFSET und errechnet aus dem Schlüssel K und der geheimen Zahl OFFSET das Verschlüsselungsergebnis V (K, OFFSET). Gemeinsam mit der Identitätskenngröße ID werden diese beiden Werte zum System S übertragen. Das System S errechnet aus der Identitätskenngröße ID mit Hilfe des festgelegten Verfahrens F1 den Schlüssel K. Das System S berechnet ebenfalls das Verschlüsselungsergebnis V (K, RNS) und vergleicht es mit dem in der Chipkarte errechneten und zum System S übertragenen Verschlüsselungsergebnis V (K, RNS). Bei positivem Vergleichsergebnis überträgt das System S ein positives Quittungssignal OK an die Chipkarte CC. Außerdem bestimmt das System mit Hilfe von K die geheime Zahl OFFSET. Nach Empfang des Quittungssignals OK sendet die Chipkarte CC eine Zufallszahl RNC zum System S. Das System S addiert zu dieser Zufallszahl RNC den Wert des OFFSET und verschlüsselt das Ergebnis der Addition. Das Verschlüsselungsergebnis V (K, [RNC+OFFSET]) wird zur Chipkarte CC übertragen und dort analog überprüft. Bei positivem Vergleichsergebnis sendet die Chipkarte CC ein positives Quittungssignal OK zum System S. Die gewünschte Anwendung ist damit freigegeben.

Die gegenseitige Authentifikation zwischen Chipkarte CC und System S verläuft dann in Fig. 2 wie folgt:
Die Chipkarte CC überträgt eine Anmeldeinformation LOG an das System S. Das System S erzeugt eine Zufallszahl RNS und überträgt diese an die Chipkarte CC. Die Chipkarte errechnet aus dem Schlüssel K und der Zufallszahl RNS ein Verschlüsselungsergebnis V (K, RNS). Außerdem bestimmt die Chipkarte den später zu verwendenden Geheimcode OFFSET und errechnet aus dem Schlüssel K und dem Geheimcode OFFSET das Verschlüsselungsergebnis V (K, OFFSET).

Das Verschlüsselungsergebnis V(K, RNS) wird zu-

sammen mit der Identitätskenngröße zum System S übertragen. Das System S errechnet aus der Identitätskenngröße ID mit Hilfe des festgelegten Verfahrens F1 den Schlüssel K. Das System S berechnet ebenfalls das Verschlüsselungsergebnis V (K, RNS) und vergleicht es mit dem in der Chipkarte errechneten und zum System S übertragenen Verschlüsselungsergebnis V (K, RNS). Bei positivem Vergleichsergebnis überträgt das System S ein positives Quittungssignal OK an die Chipkarte CC. Daraufhin überträgt die Chipkarte CC das schon berechnete Verschlüsselungsergebnis V(K, OFFSET) zusammen mit der Identitätsgröße ID. Das System quittiert wieder mit OK. Nach Empfang des zweiten Quittungssignals OK sendet die Chipkarte CC eine Zufallszahl RNC zum System S. Das System S addiert zu dieser Zufallszahl RNC den Wert der geheimen Zahl OFFSET, den das System aus dem empfangenen Wert V(K, OFFSET) berechnet hat und verschlüsselt das Ergebnis der Addition. Das Verschlüsselungsergebnis V (K, [RNC+OFFSET]) wird zur Chipkarte CC übertragen und dort analog überprüft. Bei positivem Vergleichsergebnis sendet die Chipkarte CC ein positives Quittungssignal OK zum System S. Die gewünschte Anwendung ist damit freigegeben.

In Fig. 3 wird davon ausgegangen, daß der Geheimcode OFFSET bereits zum Zeitpunkt der Initialisierung mit einem geheimen Verfahren F2 aus der Identitätskenngröße ID berechnet und analog zum Schlüssel K beim elektronischen Partner CC gespeichert wurde.

Die gegenseitige Authentifikation zwischen Chipkarte CC und System S verläuft dann in Fig. 3 wie folgt:
Die Chipkarte CC überträgt eine Anmeldeinformation LOG an das System S. Das System S erzeugt eine Zufallszahl RNS und überträgt diese Chipkarte CC. Die Chipkarte errechnet aus dem Schlüssel K und der Zufallszahl RNS ein Verschlüsselungsergebnis V (K, RNS) welches zusammen mit der Identitätskenngröße ID zum System S übertragen. Das System S errechnet aus der Identitätskenngröße ID mit Hilfe des festgelegten Verfahrens F1 den Schlüssel K. Das System S berechnet ebenfalls das Verschlüsselungsergebnis V (K, RNS) und vergleicht es mit dem in der Chipkarte errechneten und zum System S übertragenen Verschlüsselungsergebnis V (K, RNS). Bei positivem Vergleichsergebnis überträgt das System S ein positives Quittungssignal OK an die Chipkarte CC.

Nach Empfang des Quittungssignals OK sendet die Chipkarte CC eine Zufallszahl RNC zum System S.

Das System berechnet aus der vorher übertragenen Identitätsgröße ID und aus dem geheimen Verfahren F2 den Geheimcode OFFSET, addiert diesen Wert zur empfangenen Zufallszahl RNC und verschlüsselt das Ergebnis der Addition. Das Verschlüsselungsergebnis V (K, [RNC+ OFFSET]) wird zur Chipkarte CC übertragen. Die Chipkarte CC addiert zur gesendeten Zufallszahl RNC den in der Chipkarte gespeicherten Geheimcode OFFSET und führt die Verschlüsselung dieser Addition mit dem Schlüssel K durch und vergleicht das Ergebnis mit dem vom System S empfangenen Wert V(K, [RNC+OFFSET]). Bei positivem Vergleichsergebnis sendet die Chipkarte CC ein positives Quittungssignal OK zum System S. Die gewünschte Anwendung ist damit freigegeben.

Patentansprüche

1. Verfahren zur gegenseitigen Authentifikation eines eine Identitätskenngröße aufweisenden elektronischen Partners und eines Systems, auf das eine Vielzahl von elektronischen Partnern zugreifen darf, von denen jeweils mehrere gleichberechtigt in Gruppen mit gleicher Identitätskenngröße zusammengefaßt sind,

— bei dem zur Authentifikation des elektronischen Partners (CC) gegenüber dem System (S)

— das System (S) eine erste Zufallszahl (RNS) an den elektronischen Partner (CC) sendet,

— der elektronische Partner (CC) die erste Zufallszahl (RNS) mittels eines Schlüssels (K) verschlüsselt und das Verschlüsselungsergebnis zusammen mit der Identitätskenngröße (ID) an das System (S) zurücksendet,

— das System (S) zunächst anhand der Identitätskenngröße (ID) den Schlüssel (K) ermittelt und anschließend mittels dieses Schlüssels (K) aus der ersten Zufallszahl (RNS) ein Verschlüsselungsergebnis errechnet,

— das System das vom elektronischen Partner (CC) erhaltene Verschlüsselungsergebnis und das selbst errechnete Verschlüsselungsergebnis vergleicht, wobei bei Gleichheit beider Verschlüsselungsergebnisse der elektronische Partner (CC) gegenüber dem System (S) als authentisch gilt,

— und bei dem zur Authentifikation des Systems (S) gegenüber dem elektronischen Partner (CC)

— der elektronische Partner (CC) eine zweite Zufallszahl (RNC) an das System (S) sendet,

— das System (S) die zweite Zufallszahl (RNC) mittels des anhand der Identitätskenngröße (ID) des elektronischen Partners (CC) ermittelten Schlüssels (K) verschlüsselt und das Verschlüsselungsergebnis an den elektronischen Partner (CC) sendet,

— der elektronische Partner (CC) anhand der zweiten Zufallszahl (RNC) und des Schlüssels (K) ein Verschlüsselungsergebnis errechnet und

— der elektronische Partner (CC) das von dem System (S) erhaltene Verschlüsselungsergebnis und das selbst errechnete Verschlüsselungsergebnis vergleicht, wobei bei Gleichheit beider Verschlüsselungsergebnisse das System (S) gegenüber dem elektronischen Partner (CC) als authentisch gilt,

dadurch gekennzeichnet,

— daß bei der Authentifikation des Systems (S) gegenüber dem elektronischen Partner (CC)

— das System (S) sein Verschlüsselungsergebnis auf der Basis eines lediglich dem System (S) und dem elektronischen Partner (CC) bekannten erzeugten Geheimcodes (OFFSET) und der vom elektronischen Partner (CC) erhaltenen zweiten Zufallszahl (RNC) mittels des Schlüssels (K) errechnet und an den elektronischen

Partner (CC) sendet, wobei der Geheimcode (OFFSET) mit der vom elektronischen Partner (CC) gesendeten zweiten Zufallszahl (RNC) in dem System (S) mathematisch verknüpft wird,

— der elektronische Partner (CC) sein Verschlüsselungsergebnis auf der Basis des Geheimcodes (OFFSET) und der zweiten Zufallszahl (RNC) errechnet und

— der elektronische Partner (CC) das von dem System (S) erhaltene Verschlüsselungsergebnis mit dem selbst errechneten Verschlüsselungsergebnis vergleicht, wobei bei Gleichheit beider Verschlüsselungsergebnisse das System (S) gegenüber dem elektronischen Partner (CC) als authentisch gilt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Geheimcode (OFFSET) dem System (S) insbesondere in mittels des Schlüssels (K) verschlüsselter Form bei der Authentifikation des elektronischen Partners (CC) gegenüber dem System (S) übermittelt wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Geheimcode (OFFSET) dem System (S) insbesondere in mittels des Schlüssels (K) verschlüsselter Form nach der Authentifikation des elektronischen Partners (CC) gegenüber dem System (S) übermittelt wird.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Geheimcode (OFFSET) zum Zeitpunkt der Initialisierung des elektronischen Partners (CC) aus dessen Identitätskenngröße (ID) berechnet und im elektronischen Partner (CC) gespeichert wird und daß der Geheimcode (OFFSET) für die Authentifikation des Systems (S) gegenüber dem elektronischen Partner (CC) aus dessen Identitätskenngröße (ID) neu berechnet wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß der Geheimcode (OFFSET) zu der vom elektronischen Partner (CC) gesendeten zweiten Zufallszahl (RNC) in dem System (S) hinzuaddiert wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß der Geheimcode (OFFSET) durch einen Zufallsgenerator erzeugt wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß der elektronische Partner (CC) eine Chipkarte ist.

Hierzu 4 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 195 23 466 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 3. April 1997

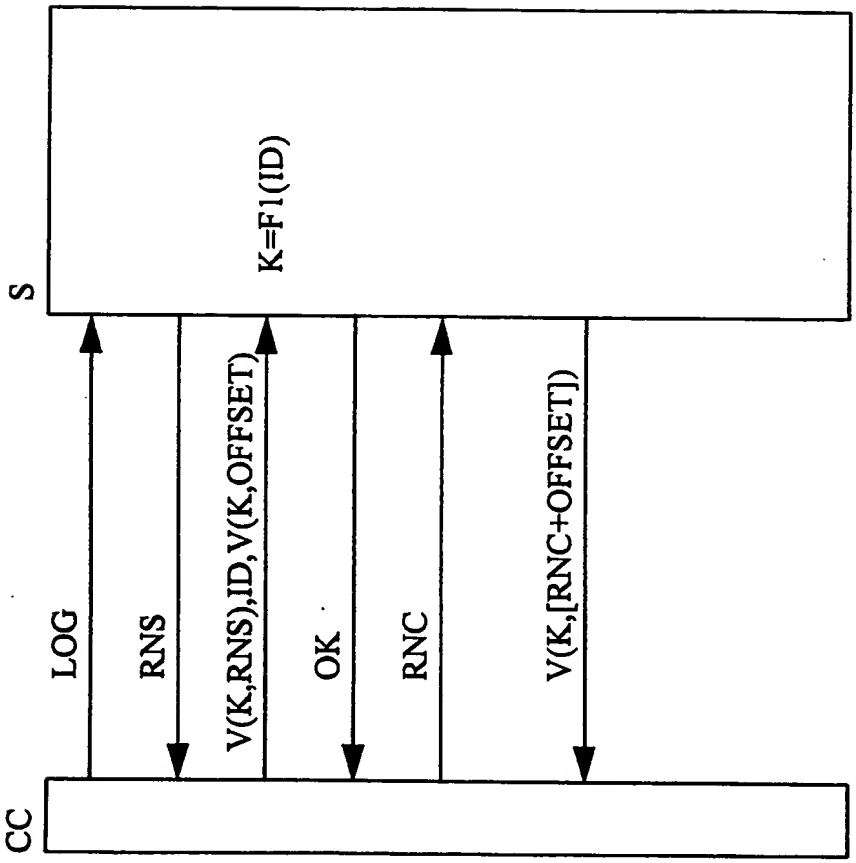


FIG 1

Nummer: DE 195 23 466 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 3. April 1997

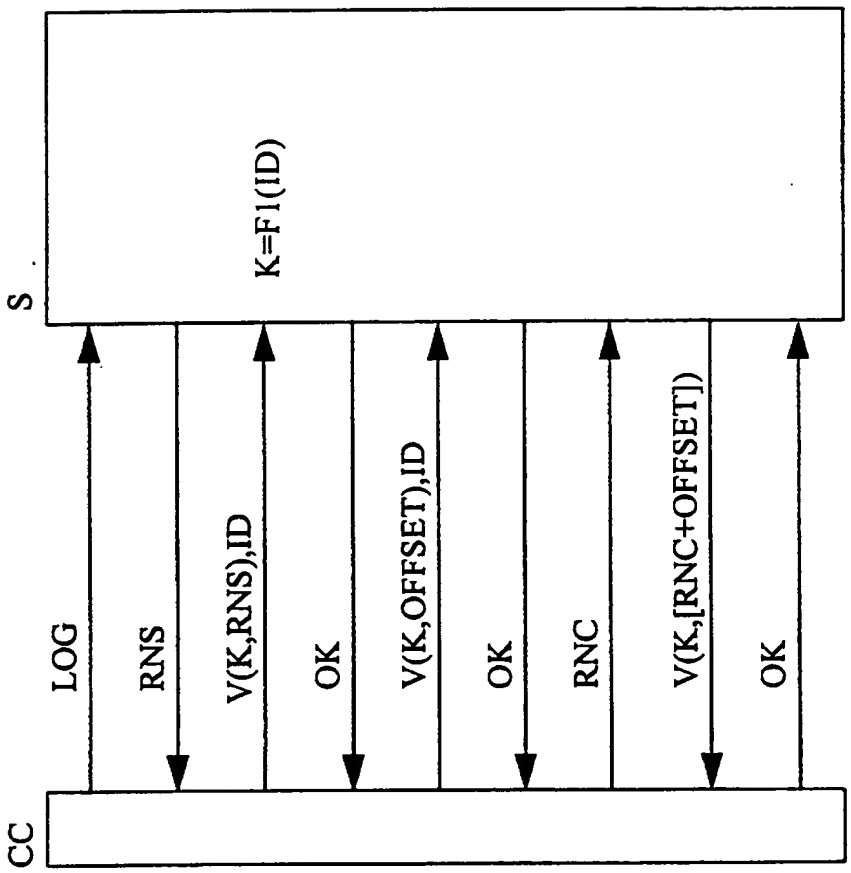


FIG 2

Nummer: DE 195 23 466 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 3. April 1997

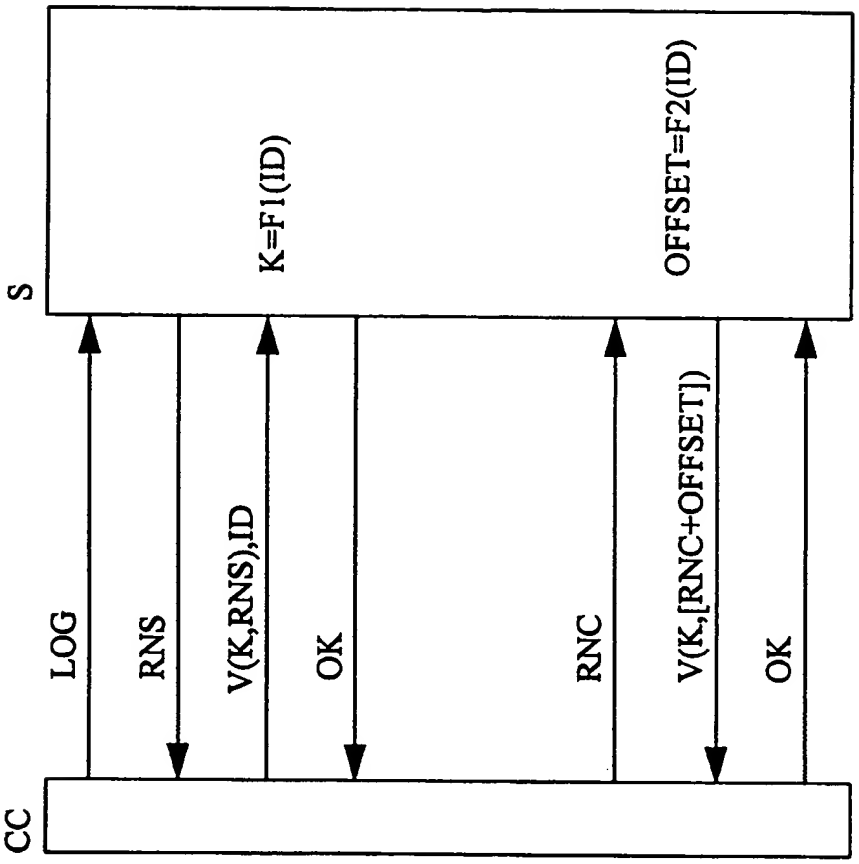


FIG 3

Nummer: DE 195 23 466 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 3. April 1997

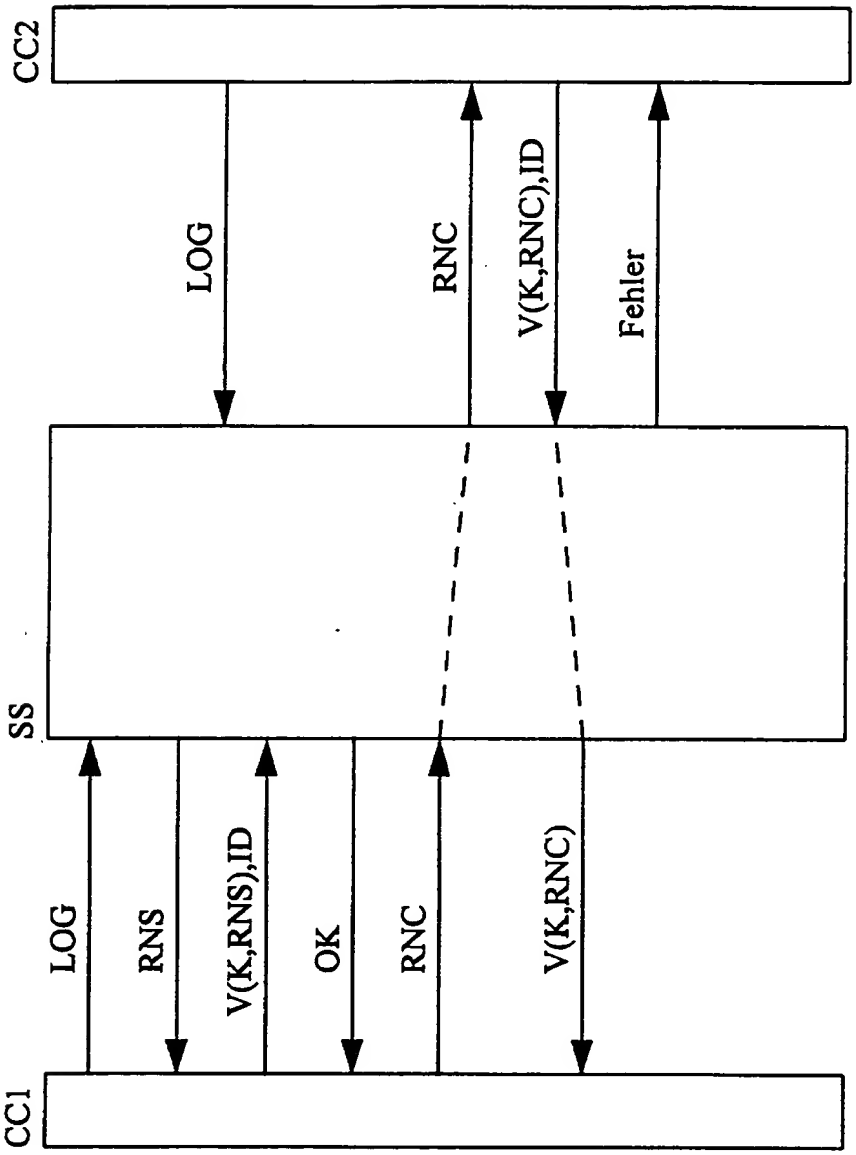


FIG 4